hewlett-packard sa3000 series vpn client deployment tool getting started guide

Hewlett-Packard Company
HP: 5971-0888
P/N: A01447-003
March 2001

Disclaimer

Information in this document is provided in connection with Hewlett-Packard Company products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Hewlett-Packard Company's Terms and Conditions of Sale for such products, Hewlett-Packard Company assumes no liability whatsoever, and Hewlett-Packard Company disclaims any express or implied warranty, relating to sale and/or use of Hewlett-Packard Company products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Hewlett-Packard Company products are not intended for use in medical, life saving, or life sustaining applications.

Hewlett-Packard Company may make changes to specifications and product descriptions at any time, without notice.

This *Hewlett-Packard SA3000 Series VPN Client Deployment Tool Getting Started Guide* as well as the software described in it is furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Hewlett-Packard Company. Hewlett-Packard Company assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Hewlett-Packard Company.

Copyright © Hewlett-Packard Company 2001.

Contents

Disclaimer iii

Getting Started
Getting Started 1-1
VPN Client Deployment Tool Components 1-2

Installing the VPN Client Deployment Tool
Before You Install the VPN Client Deployment Tool 2-1
Installing the VPN Client Deployment Tool. 2-3

Installing the VPN Client Software Files
Installing the VPN Client Software Files 3-1

Using the VPN Client Deployment Tool for the First Time
Using the VPN Client Deployment Tool for the First Time 4-1
Creating an E-mail Template File 4-2
Starting the VPN Client Deployment Tool 4-4
Logging In to the VPN Client Deployment Tool Manager 4-5
Adding a Corporation Entry 4-6
Adding a Device Entry 4-8
Adding a Tunnel Entry 4-9
Creating a Client Profile 4-11
Creating a Product Profile 4-13
Adding a User or Group Entry. 4-15

Index Index-1

Getting Started

Getting Started 1-1
VPN Client Deployment Tool Components 1-2

Getting Started

The HP SA3000 Series VPN Client Deployment Tool application allows you to deploy e-mail notifications that provide your end users with login credentials. When users access your Web server, they can download customized HP SA3000 Series VPN Client software and, after installing the client, they can access your network within minutes.

The *Hewlett-Packard SA3000 Series VPN Client Deployment Tool Getting Started Guide* provides detailed information for installing all VPN Client Deployment Tool components and setting up the VPN Client Deployment Tool for first-time use.

Note: Be sure to review the *Hewlett-Packard SA3000 Series VPN Client Deployment Tool Release Notes* before you begin the installation. After you install the application, online Help is available in the VPN Client Deployment Tool Manager to help you perform further tasks.

For more information on how to use and further set up the VPN Client Deployment Tool, see the online Help in the application. You can also view the online Help independently on your workstation or from the software CD-ROM using a browser such as Internet Explorer or Netscape Navigator.

Tasks

To install the VPN Client Deployment Tool:

1. Perform installation prerequisites.
2. Install the VPN Client Deployment Tool Manager and Database.
3. Install the VPN Client Deployment Tool Servlet on your Web server.
4. Start the VPN Client Deployment Tool Database.
5. Copy the VPN Client software (for users to download) to your computer using the Product Installation Tool.
6. Log in to the VPN Client Deployment Tool Manager.
7. Set up the VPN Client Deployment Tool for first-time use by adding a corporation entry.

VPN Client Deployment Tool Components

The VPN Client Deployment Tool consists of a manager, database, servlet, and report tool components.

VPN Client Deployment Tool Manager

The VPN Client Deployment Tool Manager is the graphical user interface (GUI) that performs the following functions:

- Captures, formats, and displays data
- Accesses deployment elements such as devices, tunnels, and users
- Lets you add, modify, or delete information entries
- Manages and controls access to the VPN Client Deployment Tool Database
- Allows only a single user to write to the VPN Client Deployment Tool Database at one time
- Scans the VPN Client Deployment Tool Database to generate the user list
- Deploys e-mail notifications

VPN Client Deployment Tool Database

The VPN Client Deployment Tool Database stores the device, tunnel, client and product profile, user, and corporation information on those users who receive e-mail notifications and HP SA3000 Series VPN Client deployments.

VPN Client Deployment Tool Servlet

To install the VPN Client Deployment Tool Servlet, your computer requires the following software configuration:

- Microsoft Windows NT 4.0 Server with Option Pack 4.0 (IIS 4.0 Web Server) or Windows 2000 Server
- Service Pack 5 (or higher) for Windows NT
- Access to SMTP mail services

The VPN Client Deployment Tool Servlet performs the following functions:

- Authenticates the remote user.

- Extracts information from the VPN Client Deployment Tool Database specific to the requesting remote user and creates the VPNCLIENT.INI and VPNUSER.INI configuration files. The configuration files are bundled with an installation or upgrade of the VPN Client into a self-extracting executable file.
- Downloads the self-extracting executable to the requesting remote user.

Report Tool Components

The VPN Client Deployment Tool comes with several extra tool components to help you make reporting data easy.

- Create Audit Report Tool

  This program creates a text file that contains a list of users who have logged in to the VPN Client Deployment Tool Web server to download the VPN Client files.

- Create User Report Tool

  This program creates a text file that contains a list of users that have been notified through the Deploy window of an available deployment.

- Purge Audit Data Tool

  This program permanently erases all audit records from the database.

Installing the VPN Client Deployment Tool

Before You Install the VPN Client Deployment Tool 2-1
Installing the VPN Client Deployment Tool. 2-5

Before You Install the VPN Client Deployment Tool

Before you can use the HP SA3000 Series VPN Client Deployment Tool on your Windows NT or Windows 2000 Server, you must install the following components:

- VPN Client Deployment Tool Manager and Database
- VPN Client Deployment Tool Servlet (The Servlet contains the necessary JRun components used by the VPN Client Deployment Tool to allow users to download HP SA3000 Series VPN Clients.)

Note: The VPN Client Deployment Tool components may be installed on either one or two computers, depending on the configuration you want to use. See "Supported Configurations" in the *Hewlett-Packard SA3000 Series VPN Client Deployment Tool Release Notes* for more information.

CAUTION: When you install or upgrade the VPN Client Deployment Tool you must reboot your Windows NT Server. To avoid additional network downtime, install the application during scheduled maintenance periods. Otherwise, your users could experience connection difficulties to your Web server.

IIS Script and Permission Types

Ensure that the IIS Script setup and permission types are configured properly.

Steps

To ensure the proper IIS Script and permission type setup:

Windows NT users:

1. Start the IIS Management Console by clicking Start and selecting Programs, Windows NT 4.0 Option Pack, Microsoft Internet Information Server, Internet Service Manager.
2. In the tree-like structure that appears in the left pane, expand the entry for the Web site that is hosting the VPN Client Deployment Tool. (This may be listed under "Default Web Site.")
3. Right-click on SCRIPTS and select Properties.
4. Select the Virtual Directory tab.

5. Ensure that the Local Path field points to the correct scripts directory. For example, `c\:Inetpub\scripts`.
6. Set Permissions to Execute (including script).

Windows 2000 users:

1. Start the Internet Information Services by clicking Start and selecting Programs, Administrative Tools, Internet Services Manager, Internet Information Services.
2. In the tree-like structure that appears in the left pane, expand the entry for the Web site that is hosting the VPN Client Deployment Tool. (This may be listed under “Default Web Site.”)
3. Right-click on SCRIPTS and select Properties.
4. Select the Virtual Directory tab.
5. Ensure that the Local Path field points to the correct scripts directory. For example, `c\:Inetpub\scripts`.
6. Set Permissions to Execute (including script).

Installing the VPN Client Deployment Tool

Steps

To install the VPN Client Deployment Tool:

1. Insert the VPN Client Deployment Tool CD-ROM into the CD-ROM drive.

   The VPN Client Deployment Tool installation program starts automatically.

   Note: If the installation program does not start automatically, select Run in the Start menu and enter `<CD-ROM drive letter>:\splash.exe` and click OK.

   The VPN Client Deployment Tool Welcome dialog box appears.

2. Click Install VPN Client Deployment Tool.

   The Setup Type window appears.

3. To automatically install the VPN Client Deployment Tool Manager and Servlet, select `Install Manager and Servlet` or if you need to install a single component, select either the `VCDT Manager` or `VCDT Servlet` entry.

Installing the VPN Client Deployment Tool Manager

If you select `Install Manager and Servlet`, the VPN Client Deployment Tool Manager is installed first. If you want to install the Servlet first or by itself, select `Install VCDT Servlet` and go to "Installing the VPN Client Deployment Tool Servlet" following this procedure.

1. In the Setup Type window, click Next.

   The VPN Client Deployment Tool Manager Welcome dialog box appears.

2. Click Next.

   The Software License Agreement dialog box appears.

3. Click Yes to accept the software license agreement.

   The Choose Destination Location dialog box appears.

4. Confirm the default destination (`C:\Program Files\HP SA3000 VPN\VPN Client Deployment Tool`) or enter another destination directory.

5. Click Next.

   The Select Program Folder dialog box appears.

6. Confirm that you want the default name VPN Client Deployment Tool added to the Program Folders or change the name to one you prefer.

7. Select to install VCDT Manager.

   The VCDT Manager software installs.

8. If you elected to install both the VPN Client Deployment Tool Manager and VPN Client Deployment Tool Servlet consecutively, click Finish to complete the Manager portion of the installation. If you installed only the VPN Client Deployment Tool Manager, select that you want to restart your computer and click Finish.

Installing the VPN Client Deployment Tool Servlet

The installation of the VPN Client Deployment Tool Servlet begins automatically after the Manager finishes (if you selected the option to install both the Servlet and Manager together).

1. The VCDT Servlet Welcome dialog box appears. Click Next.

   The Software License Agreement dialog box appears.

2. Click Yes to agree to the software license agreement.

   The Select Components dialog box appears.

3. Confirm that the JRun 2.3 is selected and click Next.

   The JRun Choose Destination Location dialog box appears.

4. Select the directory where you want JRun installed. To select the default directory, click Next.

5. Select the IIS Web Server root directory that was created when you installed IIS. To select the default directory, click Next.

   The FTP Root directory dialog box appears.

6. Select the IIS FTP root directory that was created when you installed IIS. To select the default directory, click Next.

7. Select the IIS WWW Publishing root directory that was created when you installed IIS. To select the default directory, click Next.

8. Select the IIS Web Server Scripts directory that was created when you installed IIS. To select the default directory, click Next.

   The Enter Information dialog box appears.

9. Enter the IP address of the database server. If the database server is installed on the same computer as the VPN Client Deployment Tool Manager, use the default IP address. Otherwise, enter the Database server's IP address here.

   Note: If your Manager/Database and Web server are on separate computers and you have a firewall installed between them, you must allow access to the TCP port that the Web server uses to connect to the database. By default this is port 2638.

10. Click Next.

    If you are installing JRun for the first time, the JRun Information dialog appears.

11. Click OK.

    The Setup Complete dialog box appears.

12. Select Yes, I want to restart my computer now.

13. Click Finish to restart your computer.

    The VPN Client Deployment Tool Servlet is successfully installed.

Next, you need to use the installproduct.bat utility to copy the VPN Client software to your server. See "Installing the HP SA3000 Series VPN Client Software Files" on page 3-1 for detailed information.

Installing the VPN Client Software Files

Installing the VPN Client Software Files 3-1

Installing the VPN Client Software Files

The HP SA3000 Series VPN Client software is shipped separately from the VPN Client Deployment Tool. If you want the VPN Client Deployment Tool to send customized VPN Clients to users, you must install the VPN Client software to your Windows NT or Windows 2000 Server.

The VPN Client Deployment Tool uses a copy of the VPN Client software (one of each Release you intend to deploy) along with the customized initialization files you design in the Manager to create the self-extracting executable bundle that is deployed to users.

The command-line Product Installation Utility makes this process automatic. The Product Installation Utility batch file is located, by default, in the `c:\JRun` directory and is accessed from a command prompt. You must install the VPN Client on the computer where your Manager and Database are located.

Note: To use this utility, the VPN Client Deployment Tool database must be running.

The Product Installation Utility requires both source and destination parameters to install the VPN Client Software from the CD-ROM to the Windows NT or Windows 2000 Server:

```
installproduct <source> <destination>
```

Where the <source> is the drive location of the VPN Client software, usually a CD-ROM. The <destination> parameter is the path on the Web server.

An example of a correctly formatted command-line entry appears as follows:

```
installproduct f: c:/Inetpub/ftproot/smdt
```

Steps

To install the VPN Client software:

1. Ensure that the VPN Client Deployment Tool database is running. The database starts as a service.
2. In the Start Menu, select Programs, Command Prompt.

   The command prompt window appears.
3. Type `cd jrun` to select the <drive letter>:\JRun directory.
4. Type `installproduct` with the correct <source> and <destination> parameters and press Enter.

New directories are created on your Windows NT or Windows 2000 Server and the VPN Client software files are installed.

The VPN Client files are installed into subdirectories in the root directory of your IIS FTP server (default directory `c:\Inetpub\ftproot`). At least 6 MB of disk space is required for each VPN Client installed to your hard disk.

When you have finished installing the software, you should have a directory structure similar to the one listed here:

```
c:/Inetpub/ftproot/smdt/VPN-6.80-NAM
c:/Inetpub/ftproot/smdt/VPN-6.75-INT
```

NAM indicates the North American Release of the VPN Client software. INT indicates the international release of the VPN Client. Each of the directories that are created has appropriate software subdirectories where the actual client software is located. These directories are as follows:

- client95 — indicates the Windows 95/98 compatible client
- clientNT — indicates the Windows NT compatible client
- client2k — indicates the Windows 2000 compatible client

Using the VPN Client Deployment Tool for the First Time

Using the VPN Client Deployment Tool for the First Time 4-1
Creating an E-mail Template File 4-2
Starting the VPN Client Deployment Tool 4-4
Logging In to the VPN Client Deployment Tool Manager 4-5
Adding a Corporation Entry 4-6
Adding a Device Entry 4-8
Adding a Tunnel Entry 4-9
Creating a Client Profile 4-11
Creating a Product Profile 4-13
Adding a User or Group Entry 4-15

Using the VPN Client Deployment Tool for the First Time

To use the HP SA3000 Series VPN Client Deployment Tool, you must first perform the following tasks:

Tasks

- Create an E-mail template file that contains a generic message to inform users that a new VPN Client configuration is available. See "Creating an E-mail Template File" (page 4-2).
- Start the VPN Client Deployment Tool Manager. See "Starting the VPN Client Deployment Tool" (page 4-4).
- Log in to the VPN Client Deployment Tool Manager. See "Logging In to the VPN Client Deployment Tool Manager" (page 4-5).
- Add at least one corporation entry. See "Adding a Corporation Entry" (page 4-6).
- Add at least one device entry that contains the name and IP address of a device to be assigned to a user or group. See "Adding a Device Entry" (page 4-8).
- Add at least one tunnel. You must include the device name you are going to establish a tunnel with, the tunnel name, authentication type, tunnel protocol, and port number. See "Adding a Tunnel Entry" (page 4-9).
- Add at least one client profile. You must include the client profile name, a tunnel association on the Client Profile Add/Remove Tunnels List Window, and any additional tunnel configurations. See "Creating a Client Profile" (page 4-11).
- At least one product profile. You must include a product profile description, indicate which version of the VPN Client software you want to deploy, which mode of user logon you want to use, which type of access you want to use, and you must indicate whether you want the VPN Client to be minimized upon logon. See "Creating a Product Profile" (page 4-13).
- Add at least one user or group profile to deploy information. You must include the user name, description, and a valid e-mail address. See "Adding a User or Group Entry" (page 4-15).

Creating an E-mail Template File

You can use an e-mail template file to change the format and wording of the default e-mail message that is sent to users to notify them of the deployment of a new VPN Client configuration.

The template file is a text file that you create using an ASCII text editor. It contains a generic message informs users that a new VPN Client configuration is available on the VPN Client Deployment Tool Web server.

You can customize the e-mail message for each individual user by embedding several parameters within the template file. The VPN Client Deployment Tool substitutes the appropriate values for the template parameters when it sends e-mail to the user. Parameters must be enclosed in caret (^) characters within the body of the template file. There are four e-mail template file parameters:

- ^username^

  The user's description value from the VPN Client Deployment Tool Database. If description is blank, the user's Name value is used instead.

- ^webserverurl^

  The URL of your Internet Information Server (IIS) Web server

- ^userid^

  The numeric user ID requested by the HTML login form. (Generated by VPN Client Deployment Tool)

- ^password^

  The eight-character password requested by the HTML login form. (Generated by VPN Client Deployment Tool).

Using the E-mail Template File

To use your template file:

1. Copy the e-mail template file to a directory that is accessible to the VPN Client Deployment Tool Manager.
2. Go to the Setup window in the VPN Client Deployment Tool Manager and select the corporation that you are using for deployment.
3. Enter the full path and file name of the template file in the Email Template File field

To get VPN Client Deployment Tool to deploy correctly, you must input not only the path, but also the template file name with an appropriate extension.

For example, if you store your e-mail template files in the default `C:\Program Files\HP SA3000 VPN\VPN Client Deployment Tool\Smdt\Servlet` directory, and the file name is notification.txt, you should input `C:\Program Files\HP SA3000 VPN\VPN Client Deployment Tool\Smdt\notification.txt` into the Email Template File field.

4. Click Save.

Example E-Mail Template File

Copy and modify the following e-mail template file into your text editor to create your own message.

```
Dear ^username^,

Please go to the following web page to download
the HP SA3000 Series VPN Client software:
^webserverurl^

Enter the following user id and password in the login form:

user id: ^userid^

password: ^password^

For further assistance, please contact customer
support.
```

Starting the VPN Client Deployment Tool

You must start the VPN Client Deployment Tool Manager to use the VPN Client Deployment Tool.

Prerequisites

You must install all of the software components. See preceding sections in this document.

Before you start the VPN Client Deployment Tool, ensure that IIS Admin Services are running. The VPN Client Deployment Tool Database is a part of these services and should start automatically when you start Windows NT or Windows 2000 Server.

Steps

To start the VPN Client Deployment Tool:

1. Ensure that the VPN Client Deployment Tool Database is running.

   The database is installed as a service.

2. In the Windows NT or Windows 2000 Start menu, select Programs, HP SA3000 VPN, HP SA3000 VCDT, Start Manager.

   The VPN Client Deployment Tool Login window appears.

Logging In to the VPN Client Deployment Tool Manager

You must first log in to the VPN Client Deployment Tool Manager and select a corporation to use (if more than one exists).

Prerequisite

Ensure that the Adaptive Server Anywhere database service is running. Start the VPN Client Deployment Tool Manager. See "Starting the VPN Client Deployment Tool" in the previous section of this document for more information.

Steps

To Log Into the VPN Client Deployment Tool Manager:

1. In the Login Name field, enter admin.
2. In the Password field, enter admin.

   Note: The Login Name and Password are case sensitive.
3. Click Login.

   If you already added corporation entries, the Corporation Selection dialog box appears.

   Otherwise, if this is the first time you are logging in, the Setup window appears here. You must add a corporation entry before continuing with the log in process. See "Adding a Corporation Entry" later in this document for detailed information on adding a corporation entry to the VPN Client Deployment Tool.
4. In the Corporation Selection dialog box, select a corporation entry in the drop-down list.

   Note: If only one corporation entry is defined, it is selected by default and opens automatically.
5. Click OK.

Adding a Corporation Entry

The first time you log in to the VPN Client Deployment Tool, the system requires that you create a corporation entry before you can do anything else. More corporation entries can be added later. When adding a corporation entry, you provide the corporation name, description, mail server, and Web server URL.

Prerequisite

Create an e-mail template text file. See “Creating an E-mail Template File” in the previous section.

Steps

To add a corporate entry:

1. In the left-hand navigation bar, click Setup.

   The Setup window appears.

   Note: If you are adding a corporation for the first time, the Setup window automatically appears after the initial login and the Continue Login button appears, but is disabled at this point.

2. Click Clear.
3. In the Corporation Name field, enter an abbreviated name for the corporation.

   The Corporation Name field is 1 to 8 characters.

4. In the Description field, enter the full name of the corporation.

   The Description field is 1 to 50 characters.

5. In the Mail Server IP Address field, enter the IP address of the corporation's mail server. This can be entered in numeral form (127.0.0.1) or as a domain name (mail.corporationx.com).
6. In the Port field, use the default port number.

   The default port number is 25.

7. In the Sender's Email Address field, enter the VPN Client Deployment Tool administrator's e-mail address.

   Note: You cannot deploy without a valid e-mail address in this field. An invalid address results in a false deployment.

8. In the Email Template File field, enter the absolute path where the template file for e-mail notifications reside.
9. In the Web Server URL field, enter the corporation's Web server URL. This is the IIS Web server where the VPN Client Deployment Tool servlet is installed. Users who receive e-mail notifications of updated VPN clients access this site to download the latest client.

   For example, http://<IP or web address>/smdt/index.htm
10. In the Log Level field, use the default value. The purpose of this field is to set the log level in the VPN Client. It is not a log level in the VPN Client Deployment Tool. For information on other settings for this field, see the online help for the Setup Window.
11. In the Log File field, enter the absolute path where the log file will reside.
12. In the VNICS field, enter the number of virtual network interface controllers you want the VPN Clients to be able to use.

    The default number is 2. The reason for this is when the VPN Client is installed, the default number of VNICS installed is also 2. For more information on what VNICS are and how they work within the VPN Client, see the topic “Sample vpnclient.ini File” in the VPN Client online Help. This topic discusses how to customize the VPN Client installation.
13. Click Save.

    The corporation entry you created appears in the list box, with the information you specified appearing in the appropriate columns.
14. If you are adding a corporation entry for the first time, click Continue Login to manage the currently selected corporation entry where you can add devices, tunnels, client and product profiles, users and deploy e-mail messages. Clicking Continue Login automatically takes you to the Devices window.

    Note: The Continue Login button is not enabled unless you have input the basic required information in the Setup window for your corporation.

Adding a Device Entry

You must add a device entry that contains information such as the name and IP address of an HP VPN Server Appliance SA3110/ SA3400/SA3460 devices to be assigned to a user or group. You can also add device information by polling a device and extracting its configuration information.

Steps

To add a device entry:

1. In the left-hand navigation bar, click Devices.

   The Devices window appears.

2. Click Clear.
3. In the Device Name field, enter the device host name.

   The maximum limit of the Name field is 16 characters.

4. In the Description field, enter the full description for the device.
5. In the IP Address/DNS Entry field, enter the IP address or DNS entry of the device.

   This IP address is the one that the client uses to negotiate a tunnel with the gateway device.

6. In the Automatic Device Configuration area, you may select the Device can be polled check box to automatically extract its configuration. Otherwise, go to step 10.
7. In the Poll IP Address/DNS Entry field, enter the IP address or DNS entry to be used to obtain the device configuration (typically, an IP address on the red (trusted) side of the network).
8. In the Login Name field, enter the login name for the device that is polled.
9. In the Login Password field, enter the login password for the device that is being polled.
10. Click Save.

    The device entry you created appears in the list box, with the information you specified appearing in the appropriate columns. Devices that have polling enabled appear with a plug connector symbol next to the device name.

11. Click Poll Devices to automatically populate the Tunnels section of your corporation's configuration if you have pollable devices defined.

Adding a Tunnel Entry

You must add tunnel information, including the device name, tunnel name, authentication type, tunnel protocol, and port number.

If you have a large number of tunnels, use device polling to add the information to your corporation entry. See “Adding a Device Entry” earlier in this document for more information.

Steps

To add a tunnel entry:

1. In the left-hand side navigation bar, click Tunnels.

   The Tunnels window appears.

2. Click Clear.
3. In the Device Name field, select the device name from the drop-down list.
4. In the Tunnel Name field, enter a descriptive name for the tunnel.
5. In the Authentication Type drop-down list, select the method of authentication.

   The default is VPNG.

6. Select the Multi-user check box if the tunnel you are creating is a multiuser tunnel.

   The default is a clear check box, indicating a single-user tunnel.

7. Select the WINS Tunnel check box if the tunnel is WINS capable.

   The default is a selected check box, indicating that the tunnel is WINS capable.

8. In the Tunnel Type drop-down list, select either SST (Shiva® Smart Tunneling) or IPSec.
9. In the Protocol field, enter the type of protocol you want to use to establish a tunnel.

   The default protocol is UDP.

10. In the Port field, enter the port number you want to use in conjunction with the protocol defined in the Protocol Field.

    The default port number is 2233. Port numbers 1025 through 65,535 are available.

11. In the Group/Userid Name field, enter the name of the user or group defined for that tunnel.

12. In the Challenge Phrase field, enter the challenge phrase for the device.

13. Click Save.

    The tunnel entry you created appears in the list box, with the information you specified appearing in the appropriate columns.

Creating a Client Profile

When you create a client profile, you are governing which attributes (tunnels, permissions, and so on) a group or user receives. These attributes are then set in the vpnclient.ini initialization file. This file determines how the VPN Client looks and acts after it is deployed.

Each user or group can have multiple configurations, which is important because specific users or groups may require access to several areas of your network.

Note: You may find it useful to create more than one profile where the tunnels each have different settings.

Steps

To create a client profile:

1. In the left-hand side navigation bar, click Profiles.

   The Profiles window appears.

2. Click Clear.
3. In the Profile Name field, enter a descriptive name for the profile.
4. Click Save.

   The user entry you created appears in the list box with the information you specified appearing in the appropriate columns. The Edit Profile button becomes active.

5. Click Edit Profile.

   A window appears showing you a list of tunnels you previously created.

6. Click Add/Remove Tunnels to ensure that you have assigned the correct tunnels to the client profile. If not, select the tunnel you want to add or remove and select the appropriate arrow (right-pointing arrow for assigning a tunnel to a profile, left-pointing arrow for removing a tunnel from a profile) to move the tunnel.
7. Click OK when the correct tunnel assignments have been made.
8. To configure additional tunnel settings, select the tunnel that you want to configure from the list.
9. Click Tunnel Settings.

The Tunnel Settings window appears.

Note: The Connection Type area applies to both SST and IPSec tunnels.

10. Select the Logon to Network check box if you want the users or groups to automatically log onto the network every time a tunnel connects (for example, a Windows NT domain).
11. Select the AutoConnect check box if you want your users to automatically connect to a VPN device every time the VPN Client is started.
12. In the ACL (access control list) Match Method area, select the User Identifier type you want your IPsec tunnels to use for authentication:

    Note: The ACL Match Method area is for use with IPSec tunnels only.

    - User's full email address — The client sends the user's full e-mail address as entered in the Users window for authentication (for example, jdoe@hp.com).
    - Domain — The client sends just the domain name of the user's e-mail address as entered in the Users window for authentication (for example, hp.com).
    - Other domain — Enter a domain of your choice in the field after selecting this option. Although this can be any text string or domain name, it should match an ACL rule on the VPN device. Every user or group assigned to this profile receives this domain name.
    - Certificate distinguished name — The profile uses the information in the certificate distinguished name to match an ACL rule on the VPN device. See the VPN device documentation for more information.
13. Enter the shared secret (password) for the ACL (Access Control List) on the VPN device.

Creating a Product Profile

The Product Profiles tab is where you can create and edit a product profile that lets different groups or users get different versions of the VPN Client.

Each user or group can now have multiple configurations as well. This is important because specific users or groups may require more access privileges to the VPN Client.

Steps

To create a product profile:

1. In the left-hand side navigation bar, click Profiles.

   The Profiles window appears.

2. Click the Product Profiles tab at the top of the window.
3. Click Clear.
4. In the Description field, enter a descriptive name for the profile.
5. In the VPN Version drop-down list, select the version of the VPN Client you want assigned to the product profile.

   This list only contains as many entries as there are different versions of the VPN Client you have installed in your C:\InetPub\ftproot\smdt\ directory. See *Chapter 3, Installing the VPN Client Software Files.*

6. Select the setting to specify which mode of user logon to use. The following types are available:
   - boot — This parameter indicates that the VPN Client log on is required during the Windows 95/98/2000 or Windows NT startup.
   - shell — This parameter indicates that the VPN Client log on is required after the Windows 95/98/2000 or Windows NT startup when the application is executed.
   - none — This parameter disables the logon and does not prompt the user to log on to the VPN Client software during the Windows 95/98/2000 or Windows NT boot process. This is the default mode.

7. Select which type of access you want users to have to the configuration files. The following types are available:
   - readonly — This parameter indicates that the configuration files cannot be modified in any way by the user.
   - write — This parameter indicates that the configuration file can be modified by the user. This is the default mode.
8. Select whether you want the VPN Client to be minimized upon logon. This parameter is independent of the Minimize after logon check box that appears in the VPN Client Logon window. The following switches are available:
   - yes — This parameter indicates that the client minimizes after logon. This is the default mode.
   - no — This parameter indicates that the client does not minimize after logon.
9. Click Save.

   The Product Profile description appears in the description list box on the Product Profiles tab.

Adding a User or Group Entry

You must create a user or group entry to send e-mail notifications. To add a user entry, you must provide the user name and e-mail address for each user. To add a group entry, you must first add a user and save the user as a group. Each user thereafter can be assigned to the group you just created.

Every user and group you create is a member of exactly one group, so users form a tree-like structure (similar to a file and directory structure) in the group they are in. A group can contain any number of individual users and other groups, or it can be empty.

The default group is called Everyone. If you do not specify a different group name when adding a new user, the user is added to this group.

Note: You cannot delete the Everyone group or remove its group status. You can, however, rename it to something more meaningful, such as your corporation name.

Steps

To add a user or group entry:

1. In the left-hand navigation bar, click Users.

   The Users window appears.

2. Click Clear.

3. In the User Name field, enter the identity of the user.

   For example, if user John Smith's network user name is jsmith, enter jsmith.

4. In the Description field, enter the full name of the user.

5. If you want the new user or group to inherit information from an existing group (template), click the arrow next to the Assign to Group drop-down list and select the group from which the user should inherit attributes.

   For more information on inheritance, see “Group and User Inheritance” in the online Help.

   Note: When you inherit group information from an existing group to a new user or group, the new user or group inherits the following attributes: CA (Certificate Authority) Server Name, CA Server IP Address, CA CRL Update, CA Certificate Renewal, and any tunnel assignments.

6. In the Email Address field, enter the user's e-mail address.

   This field is grayed out if you are creating a group.

7. In the Key Pair Life (days) field, enter a value for the key life.

   The default value is 365.

8. If you want to use this entry as a group for other user configurations, select the Create Group check box.

9. If you want to use an Autologon Password to bypass the VPN Client Logon authentication dialog box that appears each time the VPN Client is started, enter the password in the Autologon Password field.

10. In the Product Profile drop-down list, select the previously created product profile you want to assign to your user or group or you can use the default option. If you use the default option, the user or group receives its product profile by inheriting it from the group. See “Creating a Product Profile” earlier in this document for more information.

11. Click Save.

    The user entry you created appears in the list box with the information you specified appearing in the appropriate columns.

12. Click Assign Client Profiles to associate a previously created client profile to this group.

    The Client Profiles Assigned to Group window appears. Assign a client profile to your user or group by clicking the >> right-pointing arrow. The profile moves from the Not assigned to the Assigned list box.

13. Click OK.

14. In the Authentication area settings, click the RADIUS, SecurID, or CA (Certificate Authority) tab and do the following:

    - If you select RADIUS authentication, enter the default RADIUS user name in the Default Username field.
    - If you select CA Authentication, do the following:

    — In the Server Name field, enter a name for the Certificate Authority.

- — In the CA IP Address field, enter the Certificate Authority IP Address.
- — In the CA Certificate Name fields enter 1, 2, or 3 Certificate Authority names.
- — In the CA Challenge Phrase field, enter the challenge phrase for the Certificate Authority.
- — In the CRL Update (hours) field, enter the number of days between updates.
- — The default value is 0.
- — In the Certificate Renewal (days) field, enter the certificate renewal period in hours.
- — The default value is 0.
- If you select SecurID authentication, enter the default SecurID user name in the User Name field.

15. Click Save.

    The user entry you created appears in the list box with the information you specified appearing in the appropriate columns.

    If you need to give many users the same VPN Client configuration, you can set up one prototype user with the appropriate tunnel and Certificate Authority settings. Then, select the Create Group check box. When you assign new users to the group, they have the same configuration.

Index

A

adding
- client profiles 4-11
- corporations 4-6
- devices 4-8
- groups 4-15
- product profiles 4-13
- tunnels 4-9
- users 4-15

Audit Report Tool 1-3

B

boot logon parameter 4-13

C

client profiles 4-11
copying VPN Client 3-1
corporations
- adding 4-6
- selecting 4-5

Create Audit Report Tool 1-3
Create User Report Tool 1-3
creating
- client profiles 4-11
- e-mail template files 4-2
- product profiles 4-13

D

devices, adding 4-8

E

e-mail template files 4-2

G

getting started 1-1
groups, adding 4-15

I

IIS Scripts and Permission Types 2-1
installing 2-3
- before you install 2-1
- Manager 2-3
- overview 1-1
- Servlet 2-4
- VPN Client 3-1

installproduct.bat 3-1

L

launching VPN Client Deployment Tool. *See* starting
logging in to corporation 4-5
logging in to manager 4-5
Login Name field 4-5

M

Manager
- installing 2-3
- logging In 4-5

N

none logon parameter 4-13

O

online Help 1-1

P

parameters
- e-mail template file 4-2
- logon 4-13

Password field 4-5
prerequistites, installing 2-1
product profiles 4-13
Purge Audit Data Tool 1-3

R

Report Tool Components 1-3

S

shell logon parameter 4-13
starting VPN Client Deployment Tool 4-4
supported configurations 2-1

T

tunnels, adding 4-9

U
User Report Tool 1-3
users, adding 4-15

V
VPN Client Deployment Tool
components 1-2
database functions 1-2
Manager functions 1-2
Servlet functions 1-2
starting 4-4
using for the first time 4-1